Koncový bod Harmony

Veškerá ochrana koncových bodů, kterou potřebujete

Harmony Endpoint je kompletní řešení zabezpečení koncových bodů vytvořené pro ochranu vzdálené pracovní síly před dnešním komplexním prostředím hrozeb. Zabraňuje nejhrozivějším hrozbám pro koncový bod, jako je ransomware, phishing nebo drive-by malware, a zároveň rychle minimalizuje dopad narušení pomocí autonomní detekce a reakce.

Vaše organizace tak získá veškerou ochranu koncových bodů, kterou potřebuje, v kvalitě, kterou si zaslouží, v jediném, efektivním a nákladově efektivním řešení.

KLÍČOVÉ VÝHODY PRODUKTU

Kompletní ochrana koncového bodu: předcházejte koncovým bodům bezprostředně hrozícím hrozbám

Nejrychlejší obnova: Automatizace 90 % úloh detekce, vyšetřování a nápravy útoků

Nejlepší TCO: Veškerá ochrana koncových bodů, kterou potřebujete, v jediném, efektivním a nákladově efektivním řešení

UNIKÁTNÍ SCHOPNOSTI PRODUKTŮ

Pokročilá behaviorální analýza a algoritmy strojového učení deaktivují malware dříve, než způsobí škody

Vysoká míra úlovků a nízký počet falešných poplachů zajišťují účinnost zabezpečení a účinnou prevenci

Automatizovaná analýza forenzních dat nabízí detailní pohled na hrozby

Úplné omezení útoku a náprava pro rychlou obnovu všech infikovaných systémů

Špičkové řešení zabezpečení koncových bodů

Harmony Endpoint rozpoznán jako a Top produkt v Corporate Endpoint Ochrana pomocí AV-TEST

DALŠÍ INFORMACE

MITER ATT&CK® hodnocení

Zvýrazněte vedoucí postavení Check Point v Endpoint Security

DALŠÍ INFORMACE

Check Point Harmony Endpoint Achieve AA Hodnocení produktu v NSS Labs 2020 Advanced Test ochrany koncového bodu

ZJISTĚTE VÍCE

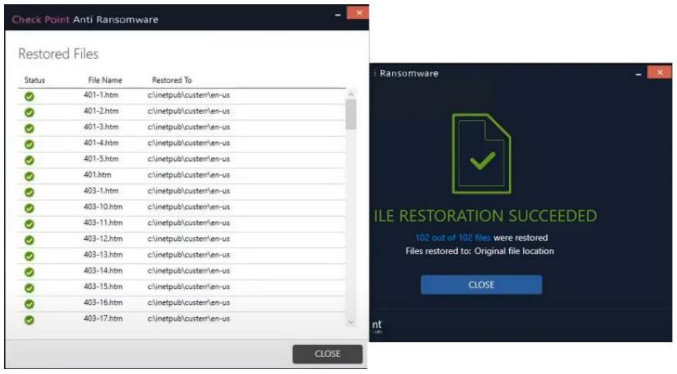
Jak to funguje

Kompletní ochrana koncových bodů

Předcházejte nejvíce bezprostředním hrozbám pro koncový bod

- Blokujte malware pocházející z procházení webu nebo e-mailových příloh dříve, než dosáhne koncového bodu, aniž by to ovlivnilo produktivitu uživatelů. Každý soubor přijatý e-mailem nebo stažený uživatelem prostřednictvím webového prohlížeče je odeslán do sandboxu emulace hrozeb, aby zkontroloval, zda neobsahuje malware. Soubory mohou být také dezinfikovány pomocí procesu Threat Extraction (technologie Content Disarm & Reconstruction), aby byl zajištěn bezpečný a vyčištěný obsah během milisekund.

- Získejte ochranu za běhu proti ransomwaru, malwaru a útokům bez souborů s okamžitou a úplnou nápravou, a to i v režimu offline.
Jakmile je detekována anomálie nebo škodlivé chování, Endpoint Behavioral Guard zablokuje a opraví celý řetězec útoků, aniž by zanechal škodlivé stopy. Anti-Ransomware identifikuje chování ransomwaru, jako je šifrování souborů nebo pokusy o kompromitaci záloh operačního systému, a automaticky automaticky obnovuje soubory zašifrované ransomwarem. Harmony Endpoint používá lokálně na stroji jedinečný prostor v trezoru, který je přístupný pouze procesům podepsaným Check Point – v případě, že se malware pokusí provést odstranění stínové kopie, stroj neztratí žádná data.



- Ochrana proti phishingu - Zabraňte krádeži pověření pomocí technologie Zero-Phishing®, která v reálném čase identifikuje a blokuje používání phishingových stránek. Stránky jsou kontrolovány a pokud jsou zjištěny škodlivé, je uživateli zablokováno zadávání přihlašovacích údajů. Zero-phishing® dokonce chrání proti dříve neznámým phishingovým webům a opětovnému použití firemních přihlašovacích údajů.

Nejlepší míra zachycení známého a zero-day malwaru v oboru

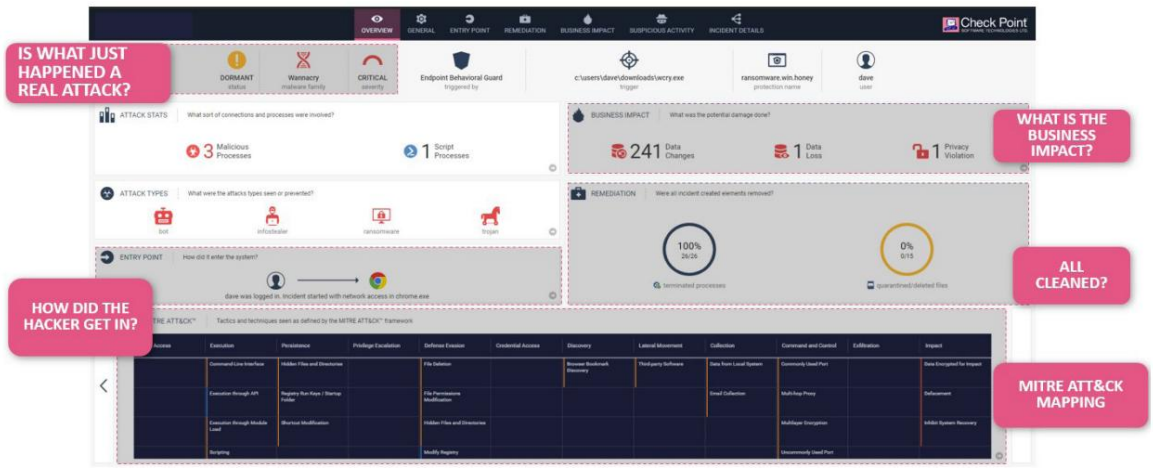
Harmony Endpoint, uznávaný lídr v oboru, jak bylo vidět v laboratorních testech AV-TEST Corporate Endpoint Protection a NSS Advanced Endpoint Protection v roce 2020, je poháněn více než 60 motory prevence hrozeb a poháněn Check Point ThreatCloud™, nejvýkonnější inteligence o hrozbách na světě pro poskytování nejvyšší celková míra zachycení hrozeb na trhu.

Nejrychlejší zotavení

Automatizace 90 % úkolů zjišťování, vyšetřování a nápravy útoků

- Automatické omezování a náprava útoků: jediné řešení Endpoint Protection, které automaticky a kompletně napraví celý řetězec kybernetického zabíjení. Jakmile je útok detekován, může být infikované zařízení automaticky umístěno do karantény, aby se zabránilo laterálnímu pohybu infekce, a obnoveno do bezpečného stavu.

- Automaticky generované forenzní zprávy: poskytující podrobný přehled o infikovaných aktivech, útočný tok, korelace s MITER ATT&CK™ Framework. Funkce Forensics automaticky monitoruje a zaznamenává události koncových bodů, včetně ovlivněných souborů, spuštěných procesů, změn systémového registru a síťové aktivity, a vytváří podrobnou forenzní zprávu. Robustní diagnostika a viditelnost útoků podporují úsilí o nápravu a umožňují správcům systému a týmům pro reakci na incidenty efektivně třídit a řešit útoky.

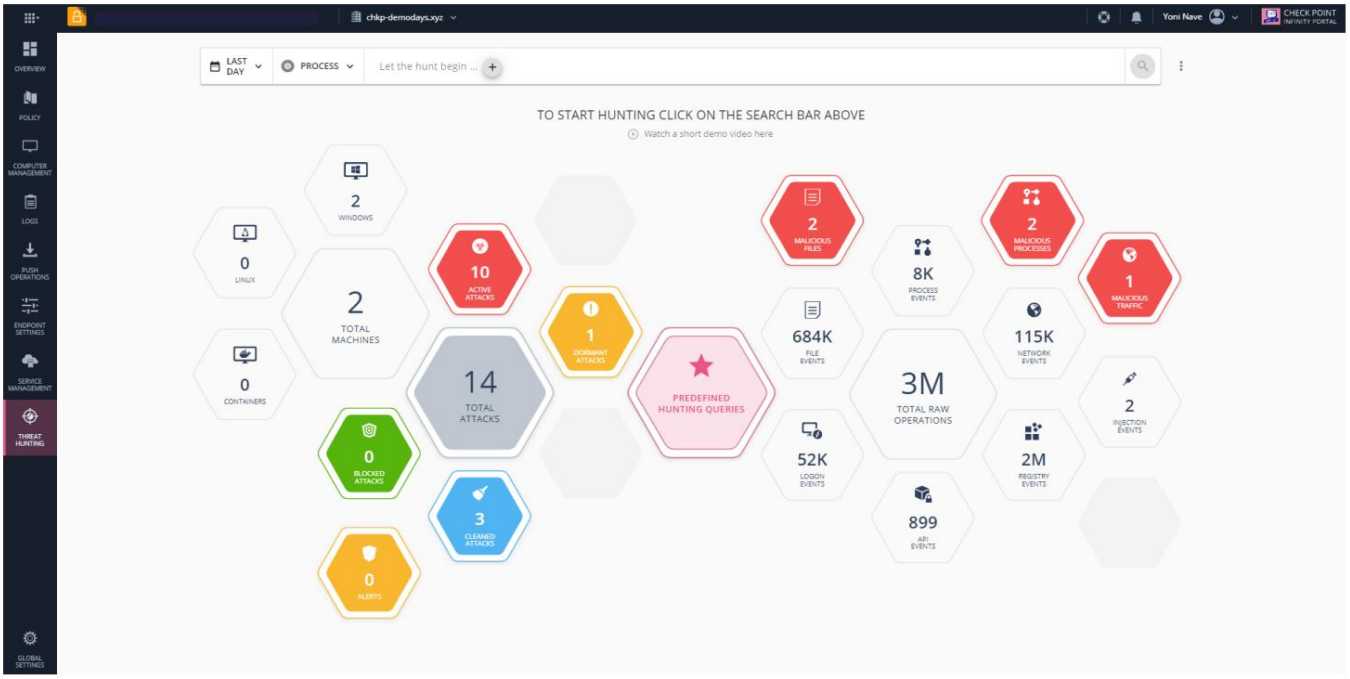


Forenzní zpráva Harmony Endpoint

„Největší výhodou používání Check Point Harmony Endpoint je, že se nemusíme obávat ransomwarových útoků na naše prostředí. Poskytuje totální klid a nemůžete na to dát cenovku. Víme, že tam bude a že naše data zůstanou v bezpečí.“

David Ulloa, ředitel informační bezpečnosti, IMC Companies

• Hledání hrozeb: díky viditelnosti v rámci celého podniku a rozšířené o globálně sdílené zpravodajství o hrozbách ze stovek milionů senzorů shromážděných ThreatCloud™. Pomocí funkce Threat Hunting můžete nastavit dotazy nebo použít předdefinované k identifikaci a prohloubení podezřelých incidentů a provádět ruční nápravná opatření.



Harmony Endpoint – Lov hrozeb

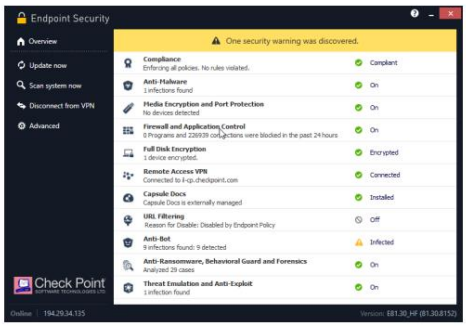
"Od té doby, co jsme nasadili Harmony Endpoint, jsme za téměř rok nezaznamenali jediný incident s pokročilým malwarem nebo ransomwarem."

Russell Walker, technologický ředitel, ministr zahraničí Mississippi

Nejlepší celkové náklady na vlastnictví

Veškerá ochrana koncových bodů, kterou potřebujete, v jediném, efektivním a nákladově efektivním řešení

Jeden jednotný agent pro ochranu EPP, EDR, VPN, NGAV, dat a procházení webu, takže vaše organizace může zefektivnit procesy a snížit celkové náklady na vlastnictví.



Plná flexibilita pro splnění vašich specifických požadavků na zabezpečení a shodu.

- Spravováno buď on-premise, nebo prostřednictvím cloudové služby, Harmony Endpoint nabízí snadno použitelné, robustní funkce a rychlé nasazení, které splní vaše požadavky
- Podpora operačních systémů Windows, macOS, Linux
- Možnost VDI (emulace desktopové instance na vzdáleném serveru), podpora VMWare Horizon, Citrix PVS/MCS
- Nedávno aktualizovaný Harmony Endpoint Installer umožňuje bezproblémové upgrady, vrácení zpět bez nutnosti restartování nebo přerušení pro koncové uživatele.
- Podpora ochrany vývojáře – pomáhá chránit vývojáře bez integrace kontinuální integrace/průběžného doručování (CI/CD) nebo integrovaného vývojového prostředí (IDE).

Staví na Check Point Infinity, první konsolidované bezpečnostní architektuře navržené k vyřešení složitosti rostoucí konektivity a nedostatečného zabezpečení, která poskytuje plnou ochranu a informace o hrozbách napříč sítěmi, cloudy, koncovými body, mobilními zařízeními a internetem věcí.

CHECK POINT INFINITY

> „Koncový bod Check Point Harmony – jediná pokročilá ochrana koncových bodů. Harmony Endpoint byl pro nás nejvhodnější Advanced Endpoint Protection. V naší celosvětové organizaci byl rychle nasazen. Konzole pro správu má intuitivní uživatelské rozhraní a snadno se používá."
>
> Sr. Security Analyst, velký globální podnik v oblasti infrastruktury

Technické specifikace

BALÍČKY HARMONY ENDPOINT	
Balíčky	• Ochrana dat – zahrnuje šifrování plného disku a šifrování vyměnitelných médií, včetně řízení přístupu a ochrany portů • Harmony Endpoint Basic – zahrnuje Anti-Malware, Anti-Ransomware, Zero-day Phishing, Advanced Threat Prevention a Endpoint Detection and Response (EDR) • Harmony Endpoint Advanced – obsahuje Harmony Endpoint Basic a navíc emulaci hrozeb a extrakci hrozeb • Harmony Endpoint Complete – zahrnuje Harmony Endpoint Advanced a zabezpečení dat (šifrování celého disku a médií) Poznámka: Soulad s koncovými body je součástí všech balíčků
OPERAČNÍ SYSTÉMY	
Operační systém	• Windows Workstation 7, 8 a 10 • Windows Server 2008 R2, 2012, 2012 R2, 2016, 2018, 2019 • MacOS Sierra 10.12, MacOS High Sierra 10.13, MacOS Mojave 10.14, MacOS BigOS 111x Mac OS Linux CatOS MacOS Ubuntu (16.04, 18.04, 20.04), Debian (9.12-10.10), RHEL (7.8-8.3), CentOS (7.8-8.3), Oracle (7.8-8.3), Amazon (2)
Content Disarm & Reconstruction (CDR) přes e-mail a web	
Extrakce hrozby	Odstraňuje zneužitelný obsah, rekonstruuje soubory za účelem odstranění potenciálních hrozeb a během několika sekund doručuje uživatelům vyčištěný
Emulace hrozeb	obsah • Schopnost sandboxingu hrozeb detekovat a blokovat nový, neznámý malware a cílené útoky nalezené v přílohách e-mailů. načtené soubory a adresy URL souborů v e-mailech. • Poskytuje ochranu napříč nejširší škálou typů souborů, včetně MS Office, Adobe PDF, Java, Flash, spustitelných souborů a archivů, např. stejně jako více prostředí Windows OS. • Odhaluje hrozby skryté v komunikaci šifrované SSL a TLS.
Centralizované řízení	
Cloud & On-Prem Management	• Harmony Service (hostováno v cloudu Check Point) • Harmony Appliance (hostováno na místě)
NGAV: Runtime Detection and Protection	
Anti-Ransomware	• Prevence hrozeb – neustále monitoruje chování specifické pro ransomware a identifikuje nelegitimní šifrování souborů, méně podpisů. • Detekce a karanténa – Všechny prvky ransomwarového útoku jsou identifikovány forenzní analýzou a poté umístěny do karantény. • Obnova dat – Šifrované soubory se automaticky obnovují ze snímků, aby byla zajištěna úplná kontinuita podnikání. • Poskytuje ochranu proti útokům založeným na exploitu, které ohrožují
Anti-Exploit	legitimní aplikace, čímž zajišťuje, že tyto zranitelnosti nemohou být pákový efekt. • Detekuje zneužití identifikací podezřelých manipulací s pamětí za běhu. • Vypne zneužitý proces při detekci jednoho, opraví celý řetězec útoků • Adaptivně detekuje a blokuje mutace malwaru podle
Strážce chování	jejich chování v reálném čase. • Identifikuje, klasifikuje a blokuje mutace malwaru v reálném čase na základě minimální podobnosti stromu provádění procesů.
Ochrana webu	
Zero-Phishing	• Ochrana v reálném čase před neznámými phishingovými stránkami • Statická a heuristická detekce podezřelých prvků na webových stránkách vyžadujících soukromé informace
Ochrana podnikových přihlašovacích údajů	Detekce opětovného použití podnikových přihlašovacích údajů na externích
Filtrování URL	webech • Odlehčený plugin prohlížeče, umožňuje/blokuje přístup k webovým stránkám v reálném čase • Prosazovat zásady organizace pro bezpečný internet pro uživatele v prostorách organizace i mimo ně, prosazovat dodržování předpisů, zlepšovat produktivita organizace • Plná viditelnost provozu HTTPS
LOV NA HROZBY	
Lov hrozeb	Shromažďování všech nezpracovaných a zjištěných událostí na koncovém bodu, umožňující pokročilé dotazy, rozbor a pivotování pro proaktivní vyhledávání hrozeb a hloubkové vyšetřování incidentů

Proč Harmony Endpoint?

Zabezpečení koncových bodů dnes více než kdy jindy hraje klíčovou roli při umožnění vzdálené pracovní síly. Vzhledem k tomu, že 70 % kybernetických útoků začíná na koncovém bodu, je nezbytná úplná ochrana koncového bodu na nejvyšší úrovni zabezpečení, aby se zabránilo narušení bezpečnosti a kompromitaci dat.

Harmony Endpoint je kompletní řešení zabezpečení koncových bodů vytvořené pro ochranu vzdálené pracovní síly před dnešním komplexním prostředím hrozeb. Zabraňuje nejhrozivějším hrozbám pro koncový bod, jako je ransomware, phishing nebo drive-by malware, a zároveň rychle minimalizuje dopad narušení pomocí autonomní detekce a reakce.

Vaše organizace tak získá veškerou ochranu koncových bodů, kterou potřebuje, v kvalitě, kterou si zaslouží, v jediném, efektivním a nákladově efektivním řešení.

Harmony Endpoint je součástí produktové sady Check Point Harmony, prvního jednotného bezpečnostního řešení pro uživatele, zařízení a přístup. Harmony sjednocuje šest produktů, aby poskytovalo nekompromisní bezpečnost a jednoduchost pro každého. Chrání zařízení a internetová připojení před nejsofistikovanějšími útoky a zároveň zajišťuje přístup nulové důvěry k podnikovým aplikacím – to vše v jediném řešení, které se snadno používá, spravuje a kupuje.

Více informací: https://www.checkpoint.com/products/advanced-endpoint-protection/

Celosvětová centrála 5
Ha'Solelim Street, Tel Aviv 67897, Izrael | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | E-mail: info@checkpoint.com

Sídlo USA 959 Skyway
Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com